IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE TO HIS MOTION FOR DISCOVERY REGARDING GOVERNMENT'S USE OF GOOGLE'S SENSORVAULT DATA

Okello Chatrie, through counsel, replies as follows to the government's response to motion for discovery regarding the government's use of Google's Sensorvault data:

I. The government has provided limited evidence in response to Mr. Chatrie's discovery request regarding the geofence information.

To date, the government has provided the following information to the defense as it relates to the data the defense has sought in its discovery motion in ECF No. 28: Excel spreadsheets with raw location data obtained from Google through execution of the geofence warrant, written communications between Google and the investigating officers in this case, and written reports from the investigating officers in this case about the geofence warrant. In its discovery motion response, the government has also indicated that its investigating officers used Microsoft Excel and Google Earth to analyze the data that Google provided pursuant to the geofence warrant. *See* ECF No. 38 at 10 n.7. Thus, the government has provided discovery in response to paragraphs 7, 11(a), and 11(b) of the discovery request in ECF No. 28. The government's response regarding the software law enforcement officials used is sufficient at this stage to satisfy the discovery request in paragraph 6 of ECF No. 28. Mr. Chatrie disputes that the government has identified in

discovery the anonymous identifier used for Mr. Chatrie's Sensorvault data in this case listed in paragraph 2 of the discovery request in ECF No. 28.

II. The government's use of Google's Sensorvault data in this case has made Google a part of the government's investigative team as it relates to the Sensorvault data.

The government's primary response to Mr. Chatrie's motion for discovery is that it does not have in its immediate possession much of the data and evidence requested. The government's response, however, fails to appreciate that how the government has used Google's Sensorvault data has made Google a part of the government's investigative team as it relates to the use of Google's location data in this case. Court have long recognized that the government's discovery obligations under Rule 16 and due process are not limited to what can be directly found in the prosecution's files. "[T]he individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case . . . ." *Kyles v. Whitley*, 514 U.S. 419, 437 (1995). "*Brady*'s commands do not stop at the prosecutor's door; the knowledge of some of those who are part of the investigative team is imputed to prosecutors regardless of prosecutors' actual awareness." *United States v. Robinson*, 627 F.3d 941, 951 (4th Cir. 2010); *see also United States v. Harry*, Cr. No. 10-1915, at *4 (D.N.M. Oct. 10, 2014) ("United States prosecutors are 'encouraged to err on the side of inclusiveness when identifying the members of the prosecution team for discovery purposes.'" (quoting Department of Justice Memorandum Regarding Guidance for Prosecutors Regarding Criminal Discovery ("Ogden memo"), authored by former Deputy Attorney General David W. Ogden, dated January 4, 2010)).

Private actors acting at the behest of the government in a criminal investigation are considered to be part of the prosecution's team for discovery purposes. For example, a nurse at a medical center who conducted an exam of a sexual assault victim is a member of the prosecution team, thus requiring the government to disclose the nurse's records. *See, e.g., McCormick v.*

Parker, 821 F.3d 1240, 1246-47 (10th Cir. 2016). Private companies providing DNA testing services on behalf of the prosecutor are also considered a part of the prosecution team. *See, e.g.*, *Bracamontes v. Superior Court of San Diego County*, 2019 WL 6044552, at *6-10 (Cal. Ct. App. Nov. 15, 2019). A private psychologist who interviewed a government witness on behalf of the prosecutor is considered a part of the prosecution team. *See, e.g.*, *State v. Ferris*, 656 S.E.2d 121, 125 (W.V. 2007). A technology company will be considered to be a part of a prosecution team where the company provided specific assistance or input on a specific case. *Cf. People v. Superior Court (Dominguez)*, 239 Cal. Rptr. 3d 71, 80 (Cal. Ct. App. 2018). The key is whether the private actor was acting at the behest of the government.

Here, that is exactly what Google was doing. The government obtained a warrant to access Google's Sensorvault data using a tiered disclosure process that Google itself designed to require warrants. Google then responded to the warrant pursuant to its process and provided data for this case. Google provided this specific information in communication with and at the behest of law enforcement officers working on this case. Google's role here, as in *McCormick*, *Bracamontes*, and *Ferris*, was as a private actor participating in a specific criminal investigation at the behest of the government. Thus, the Court must find that Google was a part of the prosecution team here as it relates to the Sensorvault data that Google provided to the government at its behest in this case. From the outset, the government would have understood that Google would not provide documentation or discovery about how its technology functions. Yet it chose to enlist Google anyways.

It is imperative for the Court to see the Hobson's choice that the government has created for Mr. Chatrie. The government utilized a complex process relying on proprietary data from a private company. This location data, and only this location data, identified Mr. Chatrie as a suspect

in this case. Because the information is proprietary, Google of course has not actually placed the data the defense has requested in the government's actual possession. Thus, the government argues that it "cannot disclose what it does not have." ECF No. 38 at 7. In reality, however, it is using Google as a one-way shield. The government is content to use the information it wants from Google but will not provide the information that the defense needs from Google to be able to assess the validity (as explained further below) of the data that Google provided.

The Sixth Amendment guarantees Mr. Chatrie the right to defend himself against the charges in this case and the right to confront and cross-examine witnesses against him. In a previous case, the government used an FBI technology specialist (the same individual that the government has relayed to the defense that it intends to rely on in this case) to testify about the validity of Google's location data using "estimations" and speculation. *See* ECF No. 48 Ex. D at 17. Such an offering cannot possibly comport with the Sixth Amendment. Because the government availed itself of this geofencing process that Google created, the burden must be on the government under due process and Rule 16 to provide the information necessary to test the validity of the data provided. Otherwise, the government must abandon its reliance on the geofencing data because its actions unreasonably infringe on Mr. Chatrie's constitutional rights.

Should, in the future, Google assert a trade secrets privilege to the data sought, the Court must view such an assertion as highly suspect when compared with the paramount constitutional rights that Mr. Chatrie holds as a criminal defendant in this case. *See DVD Copy Control Ass'n v. Bunner Inc.*, 75 P.3d 1, 15 (Cal. 2003) (explaining that the U.S. Supreme Court has "recognized that the First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance") (citing *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001); *Dun &*

Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985)); *see also Woodford*, 299 F.3d at 880 (explaining that narrow tailoring does not comport with "forc[ing the public] to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with the procedure").

III. The information that Mr. Chatrie requested is material to preparing his defense.

Mr. Chatrie has made his discovery request for the data sought in ECF No. 28 under both his right to due process and his right to discovery under Federal Rule of Criminal Procedure 16. For due process purposes, the constitution requires that the government disclose any evidence to the defendant that "is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution." *Brady v. Maryland*, 373 U.S. 83, 87 (1963). The test for materiality is whether "there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. A 'reasonable probability' is a probability sufficient to undermine confidence in the outcome." *United States v. Bagley*, 473 U.S. 667, 682 (1985). Under Rule 16, the test for materiality is whether "there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010) (quoting *United States v. Lloyd*, 992 F.2d 348, 351 (D.C.Cir.1993)); *see also* Advisory Committee Note to 1974 Amendment to Rule 16 ("broad discovery contributes to the fair and efficient administration of criminal justice . . . .").

In its response to Mr. Chatrie's motion for discovery, the government has indicated that the "anonymous identifiers" that Google provided the investigating officers were the mobile phones' "Device IDs." *See* ECF No. 38 at 3 n.1. The Device ID is a number that is unique to each phone. As Google's own help page indicates, the Device ID may be an "Identifier for Advertisers"

or an "Android Ad ID." *See* Google Ads Help: Mobile Device ID: Definition, https://support.google.com/google-ads/answer/9004555?hl=en (last visited Dec. 9, 2019). This means that each Device ID is not in fact anonymous at all, but rather it is Google tracking number assigned to individual devices that will remain the same over time. While Google did not provide actual subscriber information but for three individuals pursuant to the warrant, Google did provide at least nine unique Google tracking numbers for at least nine unique mobile phones. The Google tracking numbers showed that these individuals were in their homes, schools, and hospitals—which took very little investigation to determine. That Google tracking number will remain the same and, thus, presumably could be used in future investigations involving Sensorvault data.

The import of this revelation cannot be understated. It means that law enforcement officials misled the magistrate who issued the warrant into believing that the data Google provided pursuant to the warrant would in fact be anonymous. It may give rise to a *Franks* claim in violation of the Fourth Amendment in this case. It significantly undermines the government's assertion that the data collected from innocent users was a harmless privacy intrusion[1]. It also makes the information that the defense seeks in paragraphs 3, 4, 5, and 9 of the discovery motion in ECF No. 28 material. "[T]here is a strong indication that [the information sought about Google's collection and maintenance of Sensorvault data] will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal" at the motions hearing in this case. *Caro*, 597 F.3d at 621. Based on the defense's research and investigation to date, the defense is evaluating whether an individual has a reasonable expectation of privacy in her Google tracking number itself.

[1] As the defense can present at the evidentiary hearing, it has been fairly easy to "de-anonymize" the users of the mobile phones within the nine Google tracking numbers that Google provided in the second step of the warrant execution here—further eroding any confidence that the magistrate placed on the purported anonymity of the process the government described.

The raw data from Google that the government provided to the defense in discovery in this case also indicates that some of the Google tracking numbers connected to GPS satellites and some connected to Wi-Fi sources. A Wi-Fi source is generated by a Wi-Fi access point. A Wi-Fi access point can be a router, switch, Ethernet cable hub, or some other device that creates a wireless local area network. Mobile phones "see" these Wi-Fi access points as well as the MAC address and signal strength for each access point. The phones report this information to Google, which then—using its algorithm(s)—generates the reported locations. The phones keep a history of specific networks seen. The range of these networks is not necessarily limited to the confines of the particular building in which the network is housed. Because the Call Federal Credit Union is surrounded by a large church, a hotel, businesses, and apartment complexes (most of which would have their own individual wireless networks), it is imperative for the defense to know which Wi-Fi access points the particular Google tracking numbers connected to determine the accuracy of the location data. This information, requested in paragraph 1 of ECF No. 28, is material to the privacy intrusions and the Fourth Amendment issues raised by the geofence motion to suppress.

It is also critical for the defense to access the algorithm(s) that Google uses to determine the location of each phone. For example, one of the ways that Google generates a location for a particular phone is based on historical location data from other phones. *See* ECF No. 48 Ex. D at 32-34. When a device "sees" a Wi-Fi access point, the phone simultaneously tries to collect GPS coordinates in the area. Google collects this historical data and uses it to "locate" other phones connecting to the same Wi-Fi access point in the future. Google, and only Google, has/have the algorithm(s) that determine(s) the parameters of how Google then "locates" a particular phone at a reported place based on the historical data ***from other phones***. This information is critical, and clearly material, for the defense to be able to assess and challenge the accuracy of the purported

location data Google provided in this case. *See, e.g.*, *United States v. Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012) ("Given that the distribution charge against Buzdiak was premised on the FBI's use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense.").

Finally, the information about how law enforcement officials decided to "narrow" the 19 Google tracking numbers down to 9 and then down to 3 is critical for the defense and the Court to understand how police discretion impacted the privacy of the individuals carrying the devices with those particular Google tracking numbers. Based on the information provided to the defense in discovery in the form of raw data, it appears that the investigating officers asked for extended tracking data and even subscriber information for users whose Google tracking numbers were not even in the Call Federal Credit Union or the parking lot. Thus, the information in paragraphs 8, 10, and 11(c) of ECF No. 28 are material to preparing to cross-examine and impeach government witnesses at trial, determining which witnesses must be subpoenaed for the motions hearing, and to corroborate or rebut anticipated testimony at that hearing.

IV. The government must provide the requested information in sufficient time for the defense to be able to effectively use it at the motions hearing.

Finally, the government has indicated that if the Court orders production of the discovery that the defense has requested, it will comply with that production order under the timelines set forth in the discovery order in this case. ECF No. 38 at 1. That order, which the government drafted and presented for the defense to sign at the arraignment in this case (which was more than two weeks before the defense discovered that this case involved the geofence issue), sets deadlines for discovery production in relation to the trial in this case and not in relation to a motions hearing. ECF No. 15. The order does not make specific disclosure deadlines for information that will be material to the motions hearing in this case.

While there is no specific timeframe in which the government must produce discoverable information, it must be disclosed in time for its effective use. *See, e.g.*, *United States v. Smith Grading and Paving, Inc.*, 760 F.2d 527, 532 (4th Cir. 1985). Material information related to pretrial motions necessarily must be produced before the motions hearing. *See, e.g.*, *United States v. Wilford*, 961 F. Supp. 2d 740 (D. Md. 2013) (citing *United States v. Cranson*, 453 F.2d 123 (4th Cir. 1971)). Thus, Mr. Chatrie requests that the Court set disclosure deadlines for the government for the information sought in ECF No. 28 in relation to the motions hearing.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on December 9, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org